



مقدمة في تحليل جرائم الانترنت

الكاتب : وجدي عصام عبدالرحيم

المقالات
العلمية



تنبيه:

تعتبر هذه المقالة مشاركة من كاتبها في زيادة التوعية والمحتوى الخاص بأمن المعلومات، وقد راجعها مراجع واحد على الأقل، ولا يتحمل مركز التميز لأمن المعلومات أي تبعات لهذه المقالة، ولا أي معلومات تطرح في هذه المقالة ولا يضمن دقة المعلومة وصحتها.

مع انتشار استخدام الحواسيب وشبكة الانترنت بين المستخدمين ، تزايدت طردياً عمليات تبادل المواد الممنوعة وتزايدت عمليات الاحتيال والسرقة والابتزاز على الشبكة بين المستخدمين ، وكان لا بد من أن تبدأ المنشآت الأمنية والحكومية بالاهتمام بتخصص الأدلة الجنائية Computer Forensics حتى يمكن لتلك الجهات التحقق من الجرائم الحاصلة على الشبكة ومن مرتكبيها حتى يثبتوا إدانتهم فعلاً لكي تتم محاكمتهم مثلهم مثل المجرمين على أرض الواقع.

تخصص الأدلة الجنائية المتعلقة بالحاسب تخصص واسع وكبير ويشمل الكثير من المهارات سواء كانت في المنهجيات والأساليب المتبعة للتحقيق في جريمة أو المعرفة في تفاصيل الأنظمة وكيف تعمل من الداخل حتى يمكن للمحقق اكتشاف واسترجاع المعلومات التي يمكن أن تفيد في عملية التحقيق.

وقد لا تخلو الجرائم الحاسوبية من الاتصال بالويب والاستفادة من خدماتها مثلاً الانترنت أو البريد الإلكتروني وتبادل الملفات وخدمة المحادثات بين الأشخاص والمحادثات الهاتفية عبر الانترنت. كل من هذه الخدمات التي تقدمها لنا الويب قد تستخدم بشكل غير لائق أو بأشكال ممنوعة شرعياً، مثلاً عملية تصوير الفتيات من خلال المحادثات عبر برامج المحادثة والتي تسمح بتبادل الصور وملفات الفيديو ثم البدء بعمليات الابتزاز، أو حتى تحميل مواد ممنوعة من مواقع غير مسموح بها والبدء بالمناجزة بها، وطرق الاستخدام غير الشرعية قد لا تعد ولا تحصى.

من هنا بدأت كثير من الشركات المتخصصة في أمن المعلومات بتقديم حلول برمجية للمحققين حتى تسهل عليهم في عملهم وتيسر لهم الحصول على المعلومات وتجهيزها في أشكال قابلة للفهم من قبل المحقق حتى يقوم بفهمها واستخراج الأدلة التي تثبت فعل الجريمة. ولكن المحققين المحترفين عليهم أن يكونوا على دراية بالتفاصيل في كل ما يحققون فيه حتى يضمنوا أنهم يقوموا بعملهم في أكمل وجه، فالمحقق الذي يعمل على أنظمة الويندوز عليه بتعلم كيف يعمل ذلك النظام، وما هو نظام الملفات في ذلك النظام وكيف يعمل وأين تذهب الملفات المحذوفة فيه، والمحقق المتخصص في التعامل مع الجرائم المتعلقة بالانترنت والتي استخدمت فيها متصفحات الانترنت أو برامج المحادثة عليه معرفة كيفية استرجاع هذه المعلومات بشكل كامل من هذه البرامج وحيث أن هذه البرامج تختلف فيما بينها من الناحية الداخلية وطريقة تخزينها للمعلومات وطريقة تشفير هذه المعلومات ، فإن على المحقق دراسة كل من هذه البرامج على حده حتى يضمن أن سيقوم باسترجاع جميع المعلومات المتعلقة بالقضية.

هذه المقالة موجهة للمحققين المتخصصين في التعامل مع الجرائم المختصة بالانترنت ومتخصصين أمن المعلومات بشكل أمن والباحثين والمبرمجين في مجال الأدلة الجنائية، ولأن مجال الحديث واسع والبرامج التي تستخدم الانترنت كثيرة جداً فسيتم الحديث عن أحد البرامج التي تتعامل مع الاتصال بصفحات الانترنت (متصفح Firefox) وسيتم الحديث عن احد برامج المحادثة (برنامج Yahoo Messenger).

الغرض من هذه المقالة هو توضيح كيفية عمل هذه البرامج وخصوصاً عند تخزينها للبيانات حتى تسهل للمحقق استرجاع هذه البيانات عندما يبدأ في التحقيق. وتهدف أيضاً هذه المقالة إلى تدريب المحققين على استخدام الأساليب اليدوية في التحليل بعد فهم آليات العمل والتي قد يتطلب إليها في بعض الأحيان.

عند التحقيق في جريمة تتعلق بالاشتباه في علاقة شخص بجهة معينة وذلك من خلال البحث عن عناوين هذه الجهة في العناوين التي قام المشتبه به في دخولها، وبالرغم من أنه يمكن من خلال برامج المتصفحات نفسها أن تسترجع عناوين المواقع التي دخلها المشتبه به إلا أن هذه المعلومات لا تكفي في التحقيق، ويمكن للمحقق الحصول على المزيد من المعلومات كتاريخ زيارة الموقع المعين وعدد المرات التي زار هذه الموقع وهل يحفظ الموقع في قائمة المفضلة لديه وما هي البرامج والأدوات التي قام المشتبه به بتحميلها موثقة بتاريخ وأوقات كل من هذه العمليات، وبالرغم من أهمية هذه المعلومات إلا أن برامج المتصفحات لا تعطيها أي أهمية وتقوم بتخزين هذه المعلومات بشكل متباعد سواء في ملفات مختلفة أو في جداول مختلفة داخل قاعدة بيانات، مما يستوجب للمحقق أن يدرس طرق التخزين هذه حتى يقوم باسترجاع ما يريد من المعلومات.

أما الجرائم التي يراد أن يطلع فيها على المحادثات بين شخص مشتبه به وشخص مدان مسبقاً فإن من أهم المعلومات التي يريدها المحقق هي المحادثات نفسها بين الطرفين وأوقات جميع هذه المحادثات حتى يستطيع أن يربط بين الأحداث. المشكلة أن برامج المحادثة في الغالب تحفظ هذه المعلومات في ملفات غير معروفة البنية، أو قد يستوجب استخدام برنامج المحادثة نفسه لكي يتم قرائه تلك الملفات (مثل برنامج المحادثة من Yahoo والذي ستنم دراسته فيما بعد) لأنها تحفظ الملفات بصيغة غير معروفة إضافة إلى استخدامها لطرق من الترميز لضمان عدم فهم هذه الرسائل. لذلك على المحقق أن يستطيع فهم هذه الملفات ومعرفة بنيته حتى يستطيع استخراج المعلومات منها بكل يسر وسهولة.

استخراج المعلومات وتحليلها من المتصفح Firefox :

بدءاً من الإصدار الثالثة من متصفح فايرفوكس الشهير فقد تم تغيير طريقة تخزين المعلومات التي يخزنها المتصفح على الجهاز حيث كانت تحتفظ في ملف بصيغة mork وأصبح المتصفح يستخدم قاعدة بيانات SQLite في تخزين هذه المعلومات. وتختلف مواقع هذه الملفات باختلاف نظام التشغيل المستخدم وإصدار النظام حيث لكل نظام مواقع معروفة تستخدمها البرامج في التخزين. الأسطر التالية تبين مواقع تخزين قاعدة البيانات هذه في أنظمة التشغيل ويندوز:

Windows XP

C:\Documents and Settings\<user>\Application Data\Mozilla\Firefox\Profiles\<profile folder>\places.sqlite

Windows Vista

C:\Users\<user>\AppData\Roaming\Mozilla\Firefox\Profiles\<profile folder>\places.sqlite

قواعد البيانات هذه تكون بشكل ثنائي binary وتحتاج لكي تعرف تركيبته أن تدرس بنية هذه الملفات باستخدام أي Hex Editor أو استخدام الطريقة الأسهل وذلك باستخدام أوامر قاعدة بيانات SQLite والتي يمكن من خلالها معرفة بنية القاعدة والجداول التي بداخلها. ويمكن استخدام سطر الأوامر الذي يأتي مع القاعدة SQLite لغرض توضيح تركيبة القاعدة schema أو استخدام أي من البرامج التي تستخدم واجهة رسومية لها وذلك لتسهيل دراسة القاعدة وإيجاد المعلومات التي يمكن استخراجها منها. الشكل رقم 1 يوضح محتوى ملف قاعدة البيانات places.sqlite داخل محرر بالنظام السادس عشر.

الشكل (1) بين تركيبة قاعدة سانات متصفح فايرفوكس

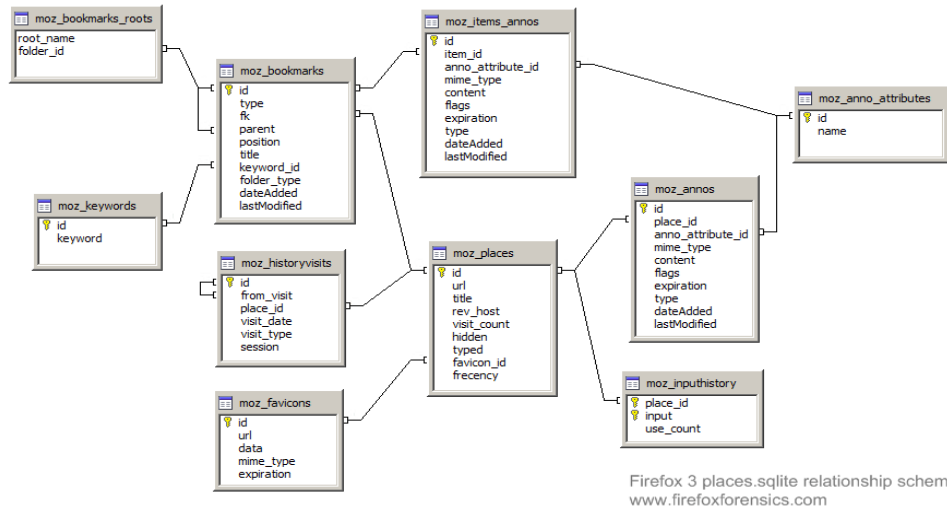
الشكل رقم 2 يوضح قاعدة بيانات places.sqlite داخل إحدى برامج توضيح تركيبة قواعد بيانات SQLite (يسمى SQLite Spy).

الشكل 2 يوضح الحدود والحقول داخل قاعدة بيانات places.sqlite

الكاتب : وجدى عصام عبدالرحيم

هذا التداخل في القاعدة وتعقيد تركيبها تجعل من الصعب أن يقوم المحقق باستخراج المعلومات منها ولو من خلال برنامج كبرنامج SQLite Spy حيث على المحقق أن يكتشف العلاقات بين هذه الجداول ويقوم باستخراج البيانات عن طريق كتابة أوامر SQL كثيرة.

الشكل رقم 3 يوضح شكل تقريبي لتركيب قاعدة البيانات places.sqlite وهي من إعداد فريق : firefoxforensics.com



الشكل (3) يوضح شكل تقريبي للجداول والعلاقات بينها في القاعدة places.sqlite

من الملاحظات على هذه القاعدة هي طريقة تخزينها للوقت والتاريخ حيث هي تخزنه بصيغة Microseconds وليس كما بقية الأنظمة والتي تستخدم seconds في تخزين الوقت (تسمى Unix-Time أو POSIX-Time وهي عدد الثواني من اليوم الأول في الشهر الأول من سنة 1970). ولتحويل من طريقة تخزين الوقت في places.sqlite إلى طريقة Unix-Time يجب القسمة على مليون وبعد ذلك يمكن استخدام الدالة datetime في SQLite والتي سوف تقوم بمهمة تحويل هذه الثواني إلى الوقت والتاريخ بشكل نصي.

الشكل (4) يوضح الاستعلام الذي يمكن من خلاله الحصول على جميع المواقع التي تمت زيارتها موضحاً وقت وتاريخ الزيارة لكل موقع.

Name	Type	NN	
main	C:\Users\Wajdy		
Tables (11)			
moz_anno_attributes			
moz_annos			
moz_bookmarks			
moz_bookmarks_roots			
moz_favicons			
moz_historyvisits			
moz_inputhistory			
moz_items_annos			
moz_keywords			
moz_places			
sqlite_sequence			
Collations (7)			


```
SELECT datetime(moz_historyvisits.visit_date/1000000,'unixepoch'), moz_places.url
FROM moz_places, moz_historyvisits
WHERE moz_places.id = moz_historyvisits.place_id
```

datetime(moz_historyvisits.visit_date/1000000,'unixepoch')	url
2010-05-28 13:03:56	https://www.google.co...
2010-05-21 23:10:14	https://www.google.co...
2010-06-25 14:25:48	https://www.google.co...
2010-05-21 23:10:28	https://mail.google.com...
2010-05-21 23:20:22	https://mail.google.com...
2010-06-02 17:37:04	https://login.live.com/p...
2010-09-21 21:34:33	https://login.live.com/p...
2010-09-21 19:05:58	https://login.live.com/p...
2010-08-07 05:24:32	https://login.live.com/p...
2010-08-06 15:02:32	https://login.live.com/p...
2010-06-04 12:29:10	https://login.live.com/p...
2010-06-04 12:29:02	https://login.live.com/p...

الشكل (4) يوضح كيفية الحصول على معلومات زيارة المواقع بعد تطبيق بعض من الاستعلامات

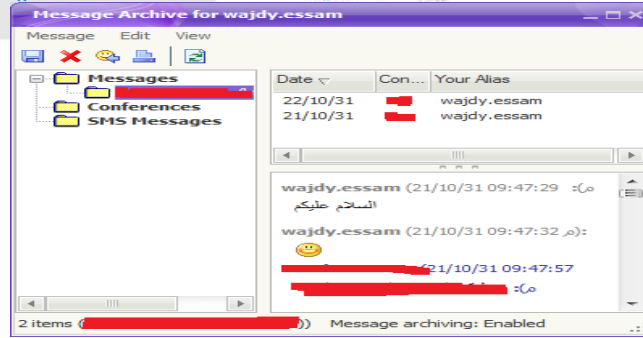
من خلال هذه الاستعلامات يمكن الحصول على جميع المعلومات المتعلقة بالمعلومات الموجودة في قاعدة بيانات المتصفح فايرفوكس، ولكن بما أن هذا يتطلب وقتاً لكتابة كل من الاستعلامات حتى يمكن الحصول على النتيجة إضافة لصعوبة تذكر هذه الاستعلامات، فإن كتابة برنامج متخصص في استرجاع هذه المعلومات بكل يسر وسهولة يعتبر أمر ضروري للمحققين حتى تساعدهم في إثبات ما يمكن إثباته على المشتبه به.

من أشهر البرامج المتخصصة في استرجاع معلومات متصفح فايرفوكس هي Firefox 3 Extractor و FoxAnalysis ووظيفة هذين البرامج مشابه لبعضها حيث تقوم باستخراج كل الزيارات التي قام بها المستخدم Histories ومفضلة المستخدم Bookmarks وملفات الكوكيز Cookies والملفات التي قام بتحميلها المستخدم Downloads ومعلومات تسجيل الدخول (اسم المستخدم وكلمات المرور إذا قام المستخدم بحفظها) Logins. إضافة إلى تزويد المحقق بخاصية البحث في تلك المعلومات وحفظ هذه المعلومات وتصديرها على شكل ملفات أكسل أو ملفات CSV.

استخراج محادثات برنامج المحادثة Yahoo Messenger :

عند إجراء المحادثات عبر برامج المحادثة Yahoo! Messenger فقد يحفظ البرنامج هذه المحادثات حتى تستطيع الرجوع إليها فيما بعد إذا احتجتها وذلك على حسب إعداداتك للبرنامج، النسخ السابقة من برنامج المحادثة Yahoo كانت خاصية الحفظ بها مفعلة بالشكل الافتراضي عند تنصيب البرنامج، بعد ذلك قامت الشركة بإلغاء خاصية الحفظ التلقائية وجعلها على حسب إعدادات المستخدم.

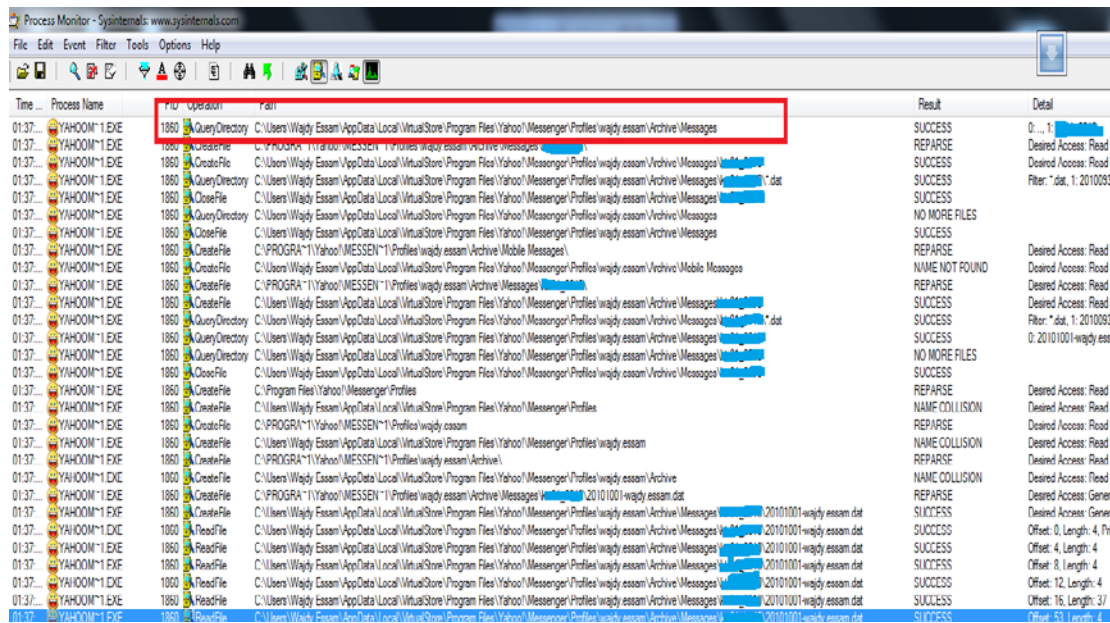
المحادثات في برنامج Yahoo Messenger لا تحفظ بشكل نصي واضح clear text ولكن تحفظ في ملفات ثنائية binary files لها بنية غير موثقة وغير معروفة والغرض من ذلك جعل هذه المحادثات غير مقروءة لأي شخص يريد الإطلاع عليها. ويستطيع المستخدم الذي نتجت منه هذه الملفات استخدام برنامج ال Yahoo Messenger نفسه لكي يقوم بالحصول على النص الواضح من هذه الملفات. الشكل 5 بين القائمة التي يمكن من خلالها الحصول على المحادثات بشكل واضح.



الشكل (5) يوضح كيف يستخرج برنامج الياهو المحادثات المسجلة

طريقة تشفير المحادثات تتم باستخدام أحد أبسط الأساليب على الإطلاق (المحادثات في برنامج Yahoo Messenger تشفر باستخدام تطبيق عملية XOR المنطقية مع اسم المستخدم) وعندما سُئل فريق العمل عن ذلك ذكروا بأن الغرض الأساسي هي سهولة حفظ المعلومات وليس الغرض تشفيرها عن المستخدم.

مواقع تخزين هذه الملفات قد تختلف باختلاف نسخة برنامج المحادثة ياهو وباختلاف نسخة نظام التشغيل المستخدم ، ففي نظام ويندوز XP فهي تخزن على المسار مختلف عن نظام التشغيل ويندوز 7 فتغيرت هذه المسارات وخزنت في مكان آخر. وأسهل طريقة يمكن أن تحصل على هذه الأماكن وذلك بالاستفادة من وجود الخاصية في برنامج Yahoo Messenger والتي تمكنه من قرائته الرسائل (كما في الشكل 5) هي عن طريق مراقبة البرنامج عند تطبيق هذا الأمر ثم تتبع ماذا يقوم به حتى يمكن الحصول على المسار. الشكل (6) يبين كيف يمكن الحصول على المسار من خلال مراقبة البرنامج باستخدام process monitor.

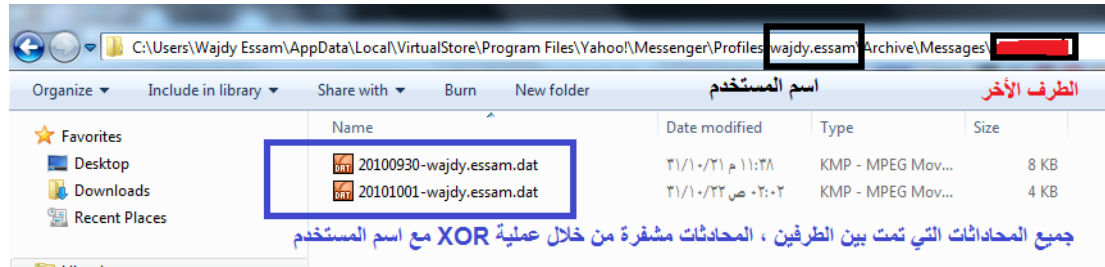


الشكل (6) يبين كيفية الحصول على مسار تخزين ملفات ال حادثة عن طريق مراقبة برنامج الياهو أثناء التسجيل

كما يتضح من الشكل فإن المسار في نظام ويندوز 7 هو التالي: C:\Users\

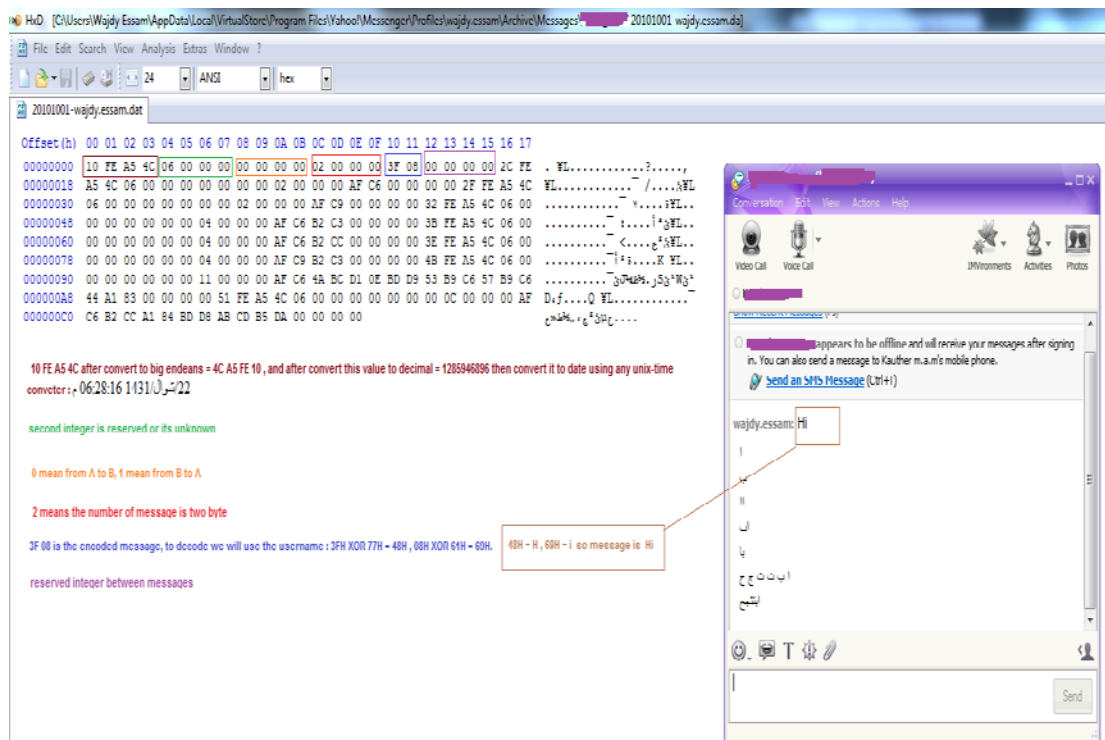
Files\Yahoo!\Messenger\Profiles\

ويتم تغيير <username> باسم المستخدم للنظام وتغيير <userid> باسم حساب المستخدم فيياهو وتغيير <buddyid> باسم حساب الطرف الآخر في المحادثة، وعند فتح ذلك المجلد سوف نجد جميع المحادثات التي تمت بين هذه الطرفين في ملفات ثنائية بالامتداد DAT. ، كل من هذه الملفات يكون اسمه مكون من تاريخ بدء المحادثة واسم المستخدم والذي سيستخدم كمفتاح في عملية فك تشفير الرسالة المخزنة.



الشكل (7) يبين المحادثات المسجلة في الجهاز

بنية هذه الملفات تتكون من : أربعة بايتات تمثل تاريخ المحادثة ويتم تخزينها ك Unix-time تليها أربعة بايت محجوزة (أو لا يعرف الغرض منها) ثم تليها أربعة بايتات أخرى توضح هل الرسالة قادمة من الطرف الأول صاحب البريد (تكون القيمة صفر) أو أنها قادمة من الطرف الآخر (تكون القيمة واحد) ثم تليها أربعة بايتات توضح عدد بايتات الرسالة (إلى هنا جميع هذه المعلومات تخزن بترميز Little Endianes) ثم تأتي بعد ذلك الرسالة ويكون عدد بايتاتها معلوم لأن الحقل الذي سبقها كان يحدد عدد بايتات الرسالة، وعندما تنتهي الرسالة تأتي أربعة بايتات أخرى تكون قيمتها صفر وذلك لكي تفصل ما بين كل رسالة ورسالة. الشكل (8) يبين كيف يمكن الحصول على الرسالة الأولى التي تم إرسالها من الطرف الأول للطرف الثاني.



الشكل (8) يبين كيف يمكن فك تشفير الرسالة للحصول على النص الأصلي الذي كتب في البرنامج

هكذا يستطيع المحققين استخراج هذه الرسائل بشكل يدوي، ولكنها عملية متعبة وتستغرق كثير من الوقت لاستخراج الرسائل وفك ترميزها وتحويل الوقت وما إلى ذلك من عمليات. لذلك اللجوء إلى البرامج التي تساعد المحققين أمر مهم جداً. هناك بعض من البرامج التي تقوم بهذه المهمة منها مجاني ومنها تجاري. ويمكن استخدام CoEIA Yahoo Decoder والذي يأتي ضمن برنامج CoEIA Forensics Toolkits والذي يستخرج جميع الرسائل وأوقات هذه الرسائل كما يوضح المرسل والمرسل إليه لكل من الرسائل.

خاتمة:

تناولت هذه المقالة عن أهمية علم الأدلة الجنائية والتحقيق في الجرائم المتعلقة باستخدام الانترنت كبرامج التصفح وبرامج المصادقة، وتناولت المقالة أساليب التحليل التي يتبعها المحللون حتى يستخرجوا المعلومات بشكل يدوي، وكمثال على ذلك تم تحليل برنامج التصفح فايرفوكس وتم استخراج المعلومات التي تفيد المحققين أثناء التحقيق في الجرائم الالكترونية، كما تم تحليل برنامج المصادقة ياهو وتوضيح كيف يمكن استخراج المعلومات والمصادقات بعد فك تشفير هذه المصادقات.

المراجع:

1. Yahoo! messenger archive file format
<http://www.0xcafefeed.com/2007/12/yahoo-messenger-archive-file-format>
2. Yahoo Messenger Protocol
<http://www.venkydude.com/articles/yahoo.htm>
3. Access Data's FTK: Internet Forensics
http://hiddenillusion.net/new-school/index.php?option=com_docman&task=doc_download&gid=6&Itemid=63